

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Jeffrey S. Bardsley et al.

Application No.: 10/624,344

Filed: July 22, 2003

For: SYSTEMS, METHODS AND DATA STRUCTURES FOR GENERATING  
COMPUTER-ACTIONABLE COMPUTER SECURITY THREAT MANAGEMENT  
INFORMATION

Confirmation No.: 7591

Group Art Unit: 2132

Examiner: F. Homayounmehr

January 14, 2008

Mail Stop Appeal-Brief Patents

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

**APPELLANTS' REPLY BRIEF UNDER 37 C.F.R. § 41.41**

This *Reply Brief* is filed pursuant to 37 C.F.R. § 41.41 to respond to the arguments raised in the *Examiner's Answer* mailed December 27, 2007. It is not believed that an extension of time and/or additional fee(s) are due. If any additional fee or extension of time is required, this should be considered a petition therefore. The Commissioner is authorized to charge any additional fee which may be required, or credit any refund, to our Deposit Account No. 09-0457.

In the Response to Arguments section of the *Examiner's Answer*, the Examiner has raised several new arguments and cited to new sections of the references that are applied in the pending rejections under 35 U.S.C. § 103. The numbered sections below provide Appellants' reply to each of the new arguments set forth in the *Examiner's Answer*. For purposes of brevity, Appellants will limit their remarks to the arguments in the *Examiner's Answer* directed to independent Claim 1.

Before responding to these new arguments, Appellants note that the *Examiner's Answer* correctly indicates that Claims 18-23 stand rejected under 35 U.S.C. § 101. Appellants are not appealing the rejections under 35 U.S.C. § 101 in light of the new guidelines issued by the United States Patent and Trademark Office in Section 2106 of the Manual of Patent Examining Procedure ("MPEP") regarding the examination of claims for patentable subject matter. Upon conclusion of the present appeal, Appellants will cancel Claims 18-23, reserving the right to pursue similar computer program product claims in a continuation application.

**I. The New Arguments Against the Rejection of Claim 1 in the Examiner's Answer**

**A. Friedrichs Does Not Disclose a TMV Having a Field Identifying at Least One System that is Affected by the Security Threat**

The July 25, 2007 *Office Action* from which the present appeal is taken ("*Office Action*") cites to paragraphs 0035 and 0042 of U.S. Patent Application Publication No. 2003/0084349 to Friedrichs et al. ("Friedrichs") as disclosing a TMV having a field that provides "identification of at least one system type that is affected by the computer security threat." (*Office Action* at 5). As shown in Appellants' *Appeal Brief*, these portions of Friedrichs discuss a database 405 that contains demographic information about the location, type and/or operating system of the security devices that uploaded information or reported a security event, and clearly do not disclose identifying the "system type that is affected by the computer security threat" as recited in Claim 1. In response to Appellants' showing, the Examiner now points to paragraph 0034 of Friedrichs, which the *Examiner's Answer* states "clearly teaches demographic information, which includes the type of system that is affected by the security threat." (*Examiner's Answer* at 12). This new argument fails for at least three independent reasons.

First, there is simply no basis to assert that the "demographic information" referred to in paragraph 0034 of Friedrichs includes information identifying "at least one system type that is affected by [a] computer security threat. As standard dictionary definitions will confirm, "demographic information" refers to the distribution, density, vital statistics, etc. of populations. Thus, the demographic information referred to in paragraph 0034 of Friedrichs is information regarding the distribution, density, vital statistics, etc. of the devices in the network. There is simply no teaching or suggestion in Friedrichs that information "identifying at least one system type that is affected by the computer security threat" would be included in such demographic information.

Second, what Claim 1 recites is a "TMV including therein a first computer-readable field that provides identification of at least one system type that is affected by the computer security threat." The demographic information discussed in paragraph 0034 of Friedrichs clearly is not part of a field of a computer actionable TMV, but instead is information stored in a database.

Third, paragraph 0034 of Friedrichs expressly states that the "demographic information" is "demographic and geographic information regarding the network providing the security event data." Thus, paragraph 0034 of Friedrichs – like paragraphs 0035 and 0042 which were cited previously by the Examiner – discusses demographic information concerning the network security devices that report security events as opposed to information identifying the "system type that is affected by the computer security threat" as recited in Claim 1.

Thus, the new argument raised in the *Examiner's Answer* fails to overcome Appellants showing that the cited references do not disclose or suggest a TMV having a first field that provides "identification of at least one system type that is affected by the computer security threat" as is recited in Claim 1.

B. Friedrichs Does Not Disclose a TMV Having a Field Identifying a Release Level for the System Type Affected

Claim 1 further recites that the TMV includes a field that provides "identification of a release level for the system type" that is affected by the computer security threat. While the *Office Action* focused on paragraph 0042 of Friedrichs as allegedly disclosing this recitation of Claim 1, the *Examiner's Answer* instead focuses on paragraph 0045 of Friedrichs, which references a product database 450 that has entries "containing vendor, product and version information for products that are vulnerable due to this flaw." Appellants respectfully submit, however, that the products database 450 of Friedrichs clearly is not a computer actionable TMV, which is what Claim 1 states must include the "identification of a release level for the system type." Accordingly, the *Examiner's Answer* also fails to rebut Appellants' showing that the cited art does not disclose a TMV having a field that provides "identification of a release level for the system type" as is recited in Claim 1.

C. Gupta Does Not Disclose Generating a Computer Actionable TMV that is Transmitted to a Plurality of Target Systems

In the *Office Action*, the Examiner argued that U.S. Patent Application Publication No. 2003/0004689 to Gupta et al. ("Gupta") disclosed "downloading the detection and protection measures to the target platform", which the *Office Action* stated met the "generating a computer-actionable Threat Management Vector (TMV)" that is transmitted "to a plurality of target systems" recitations of Claim 1. (*Office Action* at 6). As demonstrated, however, in

Appellants' *Appeal Brief*, the attack file 149 of Gupta that contains the "detection and protection measures" is not downloaded to the target systems 32 of Gupta, but instead is downloaded to a security sensor 22 that is part of the a security sensing network that is used to detect computer attacks. (See, e.g., Gupta at ¶ 0164, stating "A sensor is then supplied, through a download, with the protective software (e.g., the attack file) for the target platform").

In response to Appellants showing, the *Examiner's Answer* modifies the rejection to argue that "the sensors are associated with target platforms", and therefore downloading information to a sensor teaches downloading information to the target systems. (*Examiner's Answer* at 15). However, Appellants respectfully submit that downloading information to a sensor 22 that is part of a network 20 of computer security devices is not the same as downloading information to a target system such as the target system 32 of Gupta, and what Claim 1 expressly requires is that the information be provided (as part of a computer actionable TMV) to "a plurality of target systems for processing by the plurality of target systems." Gupta simply does not teach or disclose such a system.

Appellants' *Appeal Brief* also demonstrates that Gupta does not disclose transmitting a computer-actionable TMV to the target systems, which is what is recited in Claim 1. In response to this showing, the *Examiner's Answer* raises four counter-arguments. As shown below, none of these counter-arguments rebut Appellants showing.

First, the *Examiner's Answer* argues that Gupta at paragraph 0151 states that the attack file 149 that is transmitted to the security sensors "specifies attacks and counter measures." (*Examiner's Answer* at 15). Based on this, the Examiner states that the file "includes" countermeasures, and further states that this necessarily means that the file is computer-actionable. This logic, however, fails. In particular, a file that "specifies" countermeasures is very different from a file that "includes" countermeasures. As reference to standard dictionary definitions will confirm, to "specify" something means to mention it or describe it. It clearly does not necessarily mean that the countermeasures are "included" in the file. For example, the attack file might, for example, "specify" countermeasures by including the identification of a website which contains countermeasures or the name of a software patch that may be purchased that includes countermeasures. Such information need not be, and normally would not be, in a computer-actionable TMV. In addition, it is also clearly not inherently the case that a file that

"includes" counter measures is computer-actionable. Thus, the reference to paragraph 0151 of Gupta does nothing to overcome Appellants' showing for at least these reasons.

Second, the *Examiner's Answer* argues that paragraph 0165 of Gupta states that the methods of Gupta "constitute effective methods for operation and deployment of solutions." (*Examiner's Answer* at 16). This line from Gupta, however, clearly does not teach or disclose a computer-actionable TMV.

Third, the *Examiner's Answer* raises a completely new argument that Friedrichs at paragraph 0008 discloses generating security information by a computer and sending that information to a processor for analysis. (*Examiner's Answer* at 16). However, this argument fails for at least two reasons. First, while Friedrichs states that the information "can be uploaded to a processor", it does not state whether or not such "uploading" involves automatic uploading of computer-actionable information or manual or partially-manual uploading that involves operators. Second, and more importantly, the information referred to in Friedrichs is not a TMV that is transmitted to a plurality of target systems, but instead refers to processing that is carried out at the centralized system of Friedrichs.

Fourth and finally, the *Examiner's Answer* argues that the term "computer-actionable" covers any group of data fields. This argument likewise fails for two reasons. First, there is no teaching in Gupta that the attack file 149 is a "group of fields." It could be an e-mail message, a word processing file or any other type of file which may or may not be divided into fields. In fact, Gupta expressly states that two of the ways that the attack file 149 may be delivered are by e-mail alerts and SMS alert notifications. (Gupta at ¶ 0152). Second, the specification of the present application makes clear that the "computer-actionable TMVs" of Claim 1 are TMVs that are suitable for use by an automated threat management system. (Specification at page 9, lines 22-24; *see also* Specification at page 11, lines 7-8). There is simply no indication that the "attack file 149" of Gupta – which is often delivered by e-mail or SMS messages, comprises such a computer actionable TMV. Thus, Claim 1 is also patentable over the cited art for each of these additional reasons.

In re: Bardsley et al.  
Application No.: 10/624,344  
Filed: July 22, 2003  
Page 6 of 6

## II. Conclusion

In light of the above, Appellants submit that each of the pending claims is patentable over the cited references and, therefore, request reversal of the rejections of Claims 1-23 under 35 U.S.C. § 103.

Respectfully submitted,

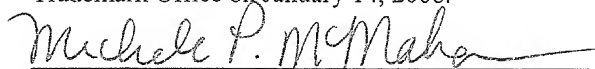


D. Randal Ayers  
Registration No. 40,493

USPTO Customer No. 20792  
Myers Bigel Sibley & Sajovec, P.A.  
Post Office Box 37428  
Raleigh, North Carolina 27627  
Telephone: (919) 854-1400  
Facsimile: (919) 854-1401

### CERTIFICATION OF ELECTRONIC TRANSMISSION UNDER 37 CFR § 1.8

I hereby certify that this correspondence is being transmitted electronically to the U.S. Patent and Trademark Office on January 14, 2008.



Michele P. McMahan

Date of Signature: January 14, 2008